Notice of Allowability	Application No.	Applicant(s)	
	09/763,271	HOFFMANN ET AL.	
	Examiner	Art Unit	
	Peter Poltorak	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *Amendment filed on 9/15/05*.

2. ☒ The allowed claim(s) is/are *1-3, 5-10 and 21-23*.

3. ☒ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☒ All b) ☐ Some* c) ☐ None of the:
      1. ☒ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☐ Information Disclosure Statements (PTO-1449 or PTO/SB/08), Paper No./Mail Date _____
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application (PTO-152)
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☒ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. This Office Action is in response to Applicant's amendment filed on 9/15/05.

2. Claims 1-3, 5, 11, 21 and 23 have been amended.

Examiner Amendment

3. An Examiner's Amendment to the record appears below. Should the changes and/or additions be unacceptable to Applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the Issue Fee.

4. The following changes were authorized (and permission to make same by Authorization for this Examiner's Amendment was given in a telephone interview with Mark J. Henry on 11/01/05).

   - In claims 1, 21 and 23 "calculating" has been changed to "producing".
   - The Preamble in claim 21 has been amended to read: "A method implemented by a computer for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:
   - In claims 21 and 23: "storing an index to be used for regenerating the private key when the private key is erased, the index indicating..."

5. The corrected version of claims 1, 21 and 23 to replace claims 1, 21 and 23 presented in the amendment filed on 9/15/05 follows at the end of this action.

Allowable Subject Matter

6. Claims 1-3, 5-11 and 21-23 are allowed.

7. The following is a statement of reasons for the indication of allowable subject matter.

8. The examiner has reconsidered the rejection cited in the previous Office Action.

9. Claims 1, 11, 21 and 23 are directed towards generating a public/private key pair and an index based on the user's input. The index and the user's input is used to regenerate the private key.

10. Although claims 21 and 23 do not explicitly teach steps of utilizing the index in the regeneration of the private key that is added to the base value, in light of the specification the examiner treats the limitation: "...storing and index to be used for regeneration the private key when the private key is erased" as an essential part of the invention. In other words, claims 21 and 23 are considered as a part of the larger process, wherein the output of the method for generating an asymmetric cryptographic key pair includes an "index" that is to be used in regeneration of the private key, and the output also includes the public and private key, as recited in the complementary claims 1 and 11.

11. The preambles of claims 1 and 11 have been given patentable weight.
The preambles help to understand the relevance of the stored index that is used in producing the regenerated private key and makes clear the significance of the index. The preamble makes it clear that the index is a value closely associated with a particular predetermined base value obtained through processing of a user entered predetermined initial value and indicating how many times the base value has been increased in order to derive a prime number. As a result it is clear that the index is

not just a product of checking whether base values are prime numbers during the users' private key generating, but it also is a value that eliminates the need to check for prime numbers during the private key regeneration.

12. The main limitation presented by applicant in the independent claims 1, 11, 21 and 23 is as follows: "receiving a user predetermined initial value entered by a user; processing the predetermined initial value to obtain a base value for obtaining the first and second prime numbers".

13. The closest found art: *Knuth* teaches checking whether a value is a prime number and, when the base value is not a prime number, increasing the value by a predetermined increment to obtain a new value, and repeating the step of checking, until a first and a second prime number are obtained *(Knuth, "Algorithm P" pg. 147).*

14. However, *Knuth* not only does not teach "receiving a predetermined initial value entered by a user" but also implementation of Knuth's method into applicant's invention would not have been obvious to one of ordinary skill in the art.

15. *Knuth's* method is directed towards finding all of the prime numbers within a set of numbers where the set starts at 1. The method starts at 1, 2 and 3 then continues to check whether the next number is prime while incrementing the number by 2. In addition *Knuth's* method (with the exception of number 2) checks only odd numbers omitting inherently non-prime even numbers.

16. As a result for the purpose of the invention *Knuth's* method would have to be significantly changed, leaving little resemblance to the original method, in order for the method to be applicable to applicant's invention.

17. Another shortcoming of the closest found art was the lack of "storing an index to obtain a stored index, the stored index being a number indicating how many times, in the step of checking, the base value has been increased until the first prime number or the second prime number are obtained" and "increasing the base value by a value determined by the index previously stored and the predetermined increment to obtain the first and second prime numbers".

18. Although keeping track of how many times the calculation has been performed is well known in the art, it would have not been obvious to one of ordinary skill in the art at the time of applicant's invention to store an index that is then used in increasing the base value used in the first and second prime number creation.

19. Another close prior art, Matyas et al. (U.S. Patent No. 5201000) refers to generation of a private key pair. Matyas et al. do not teach "storing and index indicating how many times, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained" as required by claims 1, 11, 21 and 23.

Replace claim 1 (presented in the amendment filed on 9/15/05) as follow:

--

1. A method for producing a regenerated private key by a computer for a predetermined asymmetric cryptographic key pair which includes an original private key and a corresponding public key, the regenerated private key being identical to the original private key, the original private key and the public key having been

generated by receiving a predetermined initial value entered by a user; processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers; checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value; repeating the step of checking until the first and second prime numbers are obtained; storing an index to obtain a stored index, the stored index being a number indicating how many times, in the step of checking, the base value has been increased until the first prime number or the second prime number are obtained; calculating the original private key using the first and second prime numbers; and calculating the public key using the original private key and the first and second prime numbers, the method comprising:

receiving a user input of the predetermined initial value by the computer,

processing the predetermined initial value to obtain a base value for obtaining the first and second prime numbers;

increasing the base value by a value determined by the index previously stored and the predetermined increment to obtain the first and second prime numbers; and

producing the regenerated private key using the first and second prime numbers.

--

Replace claim 21 (presented in the amendment filed on 9/15/05) as follow:

--

21. A method implemented by a computer for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:

receiving a predetermined initial value entered by a user,

processing the predetermined initial value to obtain a base value for obtaining first and second prime numbers;

checking whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value;

repeating the step of checking, until the first and second prime numbers are obtained,

storing an index to be used for regenerating the private key when the private key is erased, the index indicating how many times, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained;

producing the private key using the first prime number and the second prime number;

producing the public key using the private key, the first prime number and the second prime number, and erasing the private key.

--

Replace claim 23 (presented in the amendment filed on 9/15/05) as follow:

--

23. An apparatus for generating an asymmetric cryptographic key pair having a public key and a private key, comprising:

means for receiving a predetermined initial value entered by a user;

means for processing the predetermined Initial value to obtain a base value for obtaining first and second prime numbers;

means for checking, whether the base value is a prime number and, when the base value is not a prime number, increasing the base value by a predetermined increment to obtain a new value;

means for repeating the step of checking, until the first and second prime numbers are obtained;

means for storing an index to be used for regenerating the private key when the private key is erased, the index indicating how many times, in the step of checking, the base value has been increased until the first prime number or the second prime number is obtained;

means for producing the private key using the first prime number and the second prime number;

means for producing the public key using the private key, the first prime number and the second prime number, and

means for erasing the private key.

--

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Peter Poltorak whose telephone number is (571) 272-3840. The examiner can normally be reached from Monday through Thursday from 9:00 until 5:00, and every other Friday from 9:00 until 5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (571) 272-3838. The fax phone number for the organization where this application or proceeding is assigned is (571) 273-8300.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the Group receptionist whose telephone number is (571) 272-1600.

11/2/06

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100